REMARKS

Pursuant to applicants communication of June 6, 2001, applicants have not yet received a filing receipt. Applicants respectfully request a filing receipt.

Applicant has carefully studied the outstanding Office Action. The present amendment is intended to place the application in condition for allowance and is believed to overcome all of the rejections made by the Examiner. Favorable reconsideration and allowance of the application are respectfully requested.

Applicant has amended claims 12 - 18 to more properly claim the present invention. No new matter has been added. Claims 12 – 18 and 27 – 33 are presented for examination.

In response to the Office Action, kindly consider the following remarks:

Claim 12 has been rejected under 35 U.S.C. §102(e) as being anticipated by Nguyen, U.S. Patent No. 6,032,150 ("Nguyen").

Distinctions between Claimed Invention and U.S. Patent No. 6,032,150 to Nguyen

The present invention describes a method and system for controlling use of software. A client wishing to access protected information is sent an applet including a password by a server. When the applet requests protected information from the server, the requests include the password and the server authenticates the password before transmitting protected information. (See, for example, present specification / page 11, line 15 – page 12, line 16; original claims 12 and 27)

Nguyen describes a method and system for protecting information such as graphical elements within a web document. Nguyen uses program applets, which are created when a user tries to access the protected information, to control access to the protected information. (Nguyen / col. 1, lines 55 – 67; col. 3, lines 12 – 30; claims 1, 8 and 15) Each applet includes a unique ID, which a server associates with one or more access conditions. When

the applet executes to present protected information, it contacts the server for permission to do so. (Nguyen / col. 3, lines 31 – 39; claims 6, 13 and 19)

In contrast to the present invention in which the protected information resides on the server, the protected information of Nguyen is generated by the applet. Specifically, at col. 3, line 31 Nguyen states "*The program applet 124 is disposed to execute at the web client 110 and to present the graphical element 123 in further detail (or other further information) to the user at the web client 110.*" Additionally, claims 1, 8 and 15 of Nguyen recite "*said program applet being disposed to present said further information only upon selected conditions.*" Nguyen does not show protected information stored in a restricted-access storage area of a server, which is a feature of the present invention. (See, for example, original specification / page 11, lines 20 and 21; element 68 of FIG. 6 and FIG. 7; claim 27)

In Paragraph 10 of the Office Action, the Examiner, referring to claim 27 of the present invention, indicated that Nguyen discloses a restricted access storage area. Applicant respectfully submits that restricted access storage 68 of Applicants' FIG. 6 and FIG. 7 of the present specification refers to an area for storing protected information on server computer 64. In distinction, first region 122 in FIG. 1 of Nguyen is a region wherein protected information is generated at web client 110.

The rejection of claim 12 in the Office Action will now be dealt with specifically.

As to amended independent claim 12, applicant respectfully submits that at least the limitations in claim 12 of:

> "*receiving from said software application via said network a request for information stored in a restricted access storage area of a server*" and "*thereafter providing said information to said software application via said network while said associated password is valid*"

are neither shown nor suggested in Nguyen.

Accordingly claim 12 is deemed to be allowable.

Claims 12 – 18 and 27 – 33 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Nguyen, U.S. Patent No. 6,032,150 ("Nguyen") in view of Ananda, U.S. Patent No. 5,638,513 ("Ananda").

Distinctions between Claimed Invention and U.S. Patent No. 6,032,150 to Nguyen in view of U.S. Patent No. 5,638,513 to Ananda

Ananda describes a secure software rental system, for preventing unauthorized use of application software transferred from a server to a remote computer. The application software is modified to include header software, which carries out asynchronous dynamic password verification between the remote computer and the server while the remote computer executes the application software. As long as the password verification is successful, the application software continues to execute. Otherwise, the application software execution is terminated. (Ananda / col. 2, lines 47 – 63; col. 3, line 65 – col. 4, line 15; col. 4, line 66 – col. 5, line 4; FIG. 6; claims 1, 9, 12 and 15)

Interestingly, the present invention, Nguyen and Ananda represent three fundamentally different approaches for controlling use of software through passwords:

- The present invention delivers a software application (a program applet) and a password to a remote computer. The software application executes on the remote computer, and uses the password to request from the server protected information stored in the server.
- Nguyen delivers a software application (a program applet) and a password to a remote computer. The software application executes on the remote computer and generates the protected information, upon receiving permission from the server based on the password.
- Ananda delivers protected information (a rented software application) including a password. The software application only runs on the client computer while the password is validated by the server.

As to amended independent claim 12, applicant respectfully submits that the limitations in claim 12 of:

> "*receiving from said software application via said network a request for information stored in a restricted access storage area of a server*" and
>
> "*thereafter providing said information to said software application via said network while said associated password is valid*"

are neither shown nor suggested in Nguyen or Ananda. Applicant respectfully notes the distinction that Ananda executes the software application while the password is valid, but Ananda provides the software in advance, whether or not the password is valid. (If the password is invalid, the software application will simply not execute.)

Because claims 13 - 18 depend from claim 12 and include additional features, applicant respectfully submits that claims 13 - 18 are not anticipated or rendered obvious by Nguyen and Ananda, taken alone or in combination.

Accordingly claims 12 - 18 are deemed to be allowable.

As to independent claim 27, applicant respectfully submits that the limitations in claim 27 of:

> "*a restricted-access storage area*" and
>
> "*provide said information to said software application via said network while said associated password is valid*"

are neither shown nor suggested in Nguyen or Ananda. Applicant respectfully notes the distinction that Ananda executes the software application while the password is valid, but Ananda provides the software application in advance, whether or not the password is valid. (If the password is invalid, the software application will simply not execute.)

Because claims 28 - 33 depend from claim 27 and include additional features, applicant respectfully submits that claims 28 - 33 are not anticipated or rendered obvious by Nguyen and Ananda, taken alone or in combination.

Accordingly claims 27 - 33 are deemed to be allowable.

Respectfully submitted,
DANIEL SCHREIBER AND DAVID GUEDALIAH

Dated: 02/01/02

By: Laura Majerus

Laura A. Majerus, Reg. No. 33,417
Fenwick & West LLP
Two Palo Alto Square
Palo Alto, CA 94306
Tel.: (415) 875-2332
Fax.: (415) 281-1350

Version with markings to show changes made

Claims 12 – 18 have been amended as follows:

12. (Amended) A method for limiting the operational life of software in a network environment, the method comprising:

providing a software application with an associated password to a client via a network;

receiving from said software application via said network a request for information stored in a restricted access storage area of a server [from said software application via said network], said request comprising said associated password;

authenticating said password;

thereafter providing said information to said software application via said network while said associated password is valid; and

invalidating said password coincident with an invalidation event.

13. (Amended) A method according to claim 12 wherein said invalidating [step] comprises invalidating said password at a predetermined time.

14. (Amended) A method according to claim 12 wherein said invalidating [step] comprises invalidating said password after a predetermined elapsed time from when said request was received.

15. (Amended) A method according to claim 12 wherein said invalidating [step] comprises invalidating said password upon the detection of a loss of communication with said client.

16. (Amended) A method according to claim 12 wherein said providing [step] comprises providing said software application in the form of an applet.

17. (Amended) A method according to claim 12 wherein said providing [step] comprises providing said password assembled with said software application.

18. (Amended) A method according to claim 12 wherein said providing [step] comprises generating said password at [a] the server upon receiving said request at said server.